Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 19 (2013) 1074 – 1080

Procedia Computer Science

The 8th International Symposium on Intelligent Systems Techniques for Ad hoc and Wireless Sensor Networks (IST-AWSN)

Survey on Sensor Holes: A Cause-Effect-Solution Perspective

Nafaa Jabeur[a], Nabil Sahli[b,*], Ijaz Muhammad Khan[c]

[a]*Arab Open University, Muscat, Oman*
[b]*German University of Technology, Muscat, Oman*
[c]*Buraimi University College, Buraimi, Oman*

Abstract

We survey the sensor network holes from a cause-effect-solution perspective. We first propose a new taxonomy (PLMS) which classifies holes into type groups according to the cause of anomaly. We discuss the effects of holes on the sensor network. Finally, we survey the different curative approaches (prevention, detection, repairing, avoidance).

Keywords: wireless sensor networks; physical holes; semantic holes; logical holes; malicious hole.

1. Introduction

Sensors are small devices with limited processing and communication capabilities as well as reduced battery life. Due to these limitations, deploy-and-ignore approaches are no longer efficient. Indeed, serious problems often happen especially when sensors are operating unattended in harsh and remote areas. Holes are one challenging example of such defects. They may happen for several reasons, such as shortage of sensors' energy, sensors destruction, sensors' sleep/wakeup cycles, and data traffic congestions in some parts of the sensor network. In many cases, due to sudden external events, holes cannot be predicted. They may even extend if sensors at their boundaries are solicited with increasing data communication requests.

The monitoring of holes is a priority because of their negative –and sometimes devastating- effects on the sensor network. Detecting and repairing holes is possible. However, this is particularly challenging since typical sensor networks consist of lightweight, low-capability nodes that are unaware of their geographic locations [1]. Due to these limited capabilities, preventing holes from appearing in the sensor network or simply trying to bypass them could be a cost effective solution. A more intelligent approach to be used for monitoring holes will depend on the hole type and the current context of the sensors and the

* Corresponding author. Tel.: +968-2206-1187.
E-mail address: nabil.sahli@gutech.edu.om.

Selection and peer-review under responsibility of Elhadi M. Shakshuki
doi:10.1016/j.procs.2013.06.151

sensor network. By taking these aspects into consideration and while looking at the causes of holes, the overall performance and the lifetime of the sensor network could be improved. In this paper, we survey sensor network holes from a Cause-Effect-Solution perspective. Section 2 describes the current categorization of holes in sensor networks and then proposes alternative classifications. Section 3 proposes a new taxonomy of sensor holes which is based on the causes of anomaly and is more exhaustive. Section 4 discusses the effects of holes and Section 5 surveys the four curative approaches (prevention, detection, repairing, and avoidance) to address the problem of holes in sensor networks.

2. Categorization of Sensor Network Holes

To our knowledge, the current literature does not provide a general definition of holes in sensor networks. In contrast, it suggests a classification of these holes into types and then defines each type apart.

Ahmed et al. [2] have described four categories of holes: *coverage holes*, *routing holes*, *jamming holes, and sink/worm holes*. *Coverage holes* usually occur due to the random deployment of sensor nodes [3]. According to [4], the existence of such type of holes depends on the required degree of coverage for any given application. Indeed, the authors have stated that no *coverage hole* exists in a given area if every point in that area is covered by at least k sensors, where k is the required degree of coverage. According to [2], *routing holes* appear in an area where sensor nodes are not available or the available nodes cannot participate in data routing due to malfunctioning, battery depletion, or destruction by an external event.

In contrast with *coverage holes* and *routing holes*, *jamming holes*, *sink holes, and worm holes* result from unusual behaviors of some objects or sensors within the sensor network. Indeed, *jamming holes* occur when an object to be tracked is equipped with a device capable of jamming the radio frequency being used for communication among the sensor nodes. In spite of being able to detect the presence of the object, sensors in the vicinity are unable to communicate the information back to the sink [2]. *Sink holes* are caused by malicious nodes which try to attract the traffic within a given sensor network to a compromised node. In this attack, an adversary node seduces neighboring sensors by advertising optimized routes to forward data to the sink. The malicious node will be selected as the best next-hop by sensors in the vicinity and might be recommended to other sensor nodes. In this case, data communication will flow more and more through the malicious node that can drop data, selectively forward data based on some malicious filtering mechanism, or change data content before relaying it [5]. In addition to prevaricating the traffic, sink holes may result in congestion, which could accelerate the energy depletion of sensors which are close to the malicious node. Furthermore, like sink holes, worm holes result from malicious behaviors of some nodes in the area covered by the sensor network. Indeed, malicious nodes located in different parts of the sensor network may create a tunnel among them and start forwarding packets received at one part of the network to the other end of the tunnel by using a separate communication radio channel [2]. Consequently, nodes located in different parts of the network would believe that they are neighbors, resulting in incorrect routing convergence [2].

The current literature does not provide a rich categorization of holes in sensor networks. We thus aim at investigating the possible categorizations depending on a variety of parameters and characteristics. For instance, holes may be categorized with respect to their:

- Mobility (moving or static): In contrast with static holes caused by anomalies affecting static sensor nodes, moving holes may be caused by mobile sensors. Indeed, while moving, sensors may affect the topology of the sensor network by creating new connections and breaking others.
- Life time (persistent or temporary): Persistent holes could not be healed. They often result from intrinsic problems to sensors such as energy depletion or extrinsic events such as heavy rain or wildfire. Temporary holes (e.g., when nodes sleep), in contrast, are of limited duration and disappear/regress as their causes disappear/regress or recovery actions are performed.

- Purposes (intentional or unintentional): Unintentional holes occur when, for example, some sensors accidentally lack physical capabilities. Intentional holes are created when, for instance, some sensors go to sleep as scheduled to save energy.
- Affected function (functional or nonfunctional): Basically, a sensor node could be requested to perform sensing, processing, and/or communicating tasks. We call these tasks functional. In contrast, criteria which can be used to judge the performance and the quality of a given node, such as security or accuracy, are nonfunctional tasks. (Non)functional holes refer to (non)functional tasks.
- Cause of anomaly (Physical/semantic/logical/malicious): The most known causes are physical defects (routing and coverage holes) and malicious behaviors (jamming and sink/worm holes). Nevertheless, we believe that holes may also be caused by semantic or logical defects. We thus propose another categorization of WSN holes which includes four types of holes, namely, physical holes, semantic holes, logical holes, and malicious holes. More details on this categorization (that we name PLMS) will be given in the next section.

Based on the different categorizations cited above, we propose the following generic definition of a sensor network hole: "A hole is a static or moving, intentional or intentional, temporary or persistent anomaly in one or more functional or non-functional tasks in one or more nodes of a specific part of a sensor network". To the extent of our knowledge, this is the first attempt to define the concept of holes in sensor networks. This definition includes all the attributes that we have identified previously and which characterize any sensor network hole. The attributes indicating the causes of holes (physical, logical, malicious, or semantic) are omitted from the definition for the sake of simplicity and also because they are overlapping with the two more generic attributes which are "functional or nonfunctional".

3. PLMS: a Cause-based Taxonomy

The four different categorizations we presented above are related to different aspects of sensor holes. As in this paper we study sensor holes from a cause-effect-solution perspective, we will focus on the cause-based categorization that we named Physical/Logical/Malicious/Semantic (PLMS) taxonomy.

Physical holes: They could be classified into five types, namely, processing, energy, coverage, routing, and sensing (Fig.1-a). Processing holes may happen if in a given area of interest sensors do not have enough physical capabilities to process a given data. This is particularly due to the limited capacities of the processor. Sensor nodes which are at the origin of processing holes may cause long delays in the overall routing, sensing, or processing activities. In the case of high processing loads, the resources of those sensors could be exhausted and thus energy holes could appear. Energy holes resulting from an excessive consumption of energy could also be created when nodes, which are sharing common sensing tasks, operate simultaneously in a high density network. In Fig.1.a, we give the example of a node A which is receiving multiple and different requests. Due to its limited capabilities, node A may exhaust its energy before being able to answer all the requests and therefore an energy hole could be created. In addition to the routing holes and coverage holes we explained in Section 2, the network could have sensing holes. These holes happen due to the limited sensing ranges of some deployed sensors. In Fig.1.a, the sensor nodes B, C, and D could be able to cover the area where they are deployed. However, if they are asked to collect data from that area, they will fail since their sensing ranges are not enough wide.

Semantic holes: As the ultimate goal of the sensor network is to provide users with the right data at the right time using the right sensors [6], nodes should have certain "understanding" (or intelligence) of the content of the data they sense, process and forward. Semantic holes are basically related to the content of the collected, processed, and routed data as well as to the services provided by the sensor network. According to our literature review, the present work emphasizes on issues related to semantics since the ultimate goal of the sensor network is to provide users with the right data at the right time using the right sensors. To this end, we list four types of semantic holes (Fig.1.b). Sensor type holes could happen when

a sensor network including several types of sensors is not able to collect a specific data type from a given area. In Fig.1.b, we highlight a sensor type hole where the network is not able to collect data of type 2 and type 3 since specialized sensors are not available in the delimited area. When appropriate sensors are available, the requested data could be collected if physical impediments do not prevent this operation. However, in some circumstances, the collected data may lack accuracy or do not include the requested level of details. In such cases, we say that there is an accuracy hole. Moreover, in some configurations, the network could be deployed to provide multiple services. In such cases, subsets of sensors could be operating simultaneously to provide different services. When a given subset of sensors is not able to fulfill its task due to any type of holes, we say that there is a service hole. In such situations, neighboring sensors could be available and may help in preventing the disconnection of the service. However, these sensors could be assigned to other services and thus their support could be delayed. This happens in a collaborative architecture where sensors have to help each other depending on their availability and priorities. We illustrate in Fig.1.b an example of service holes where Service 1 is disconnected because of the absence of sensors assigned to this service in the delimited area. This hole could be healed in a sensor network with a collaborative architecture. However, it will not be healed in a sensor network with a competing architecture since sensor nodes are only dedicated to the services to which they are assigned. Fig.1.b illustrates two kinds of competition holes. The first competition hole happens when two services are using common sensors, in which case delays may result from concurrent processing. The second competition hole happens when a service like Service 3 is using exclusively some sensors in a way they disconnect another service, which is in the case of Fig.1.b Service 1.

Logical holes: Several approaches are based on dividing the sensor network into several clusters. These clusters are a logical repartition of the network depending on some criteria. We say that there is a cluster hole if a sensor is not able to get support from any neighboring peer belonging to the same cluster.

Malicious holes: In addition to jamming holes, sink holes, and worm holes outlined in Section 2, we list trust holes as part of malicious holes (Fig.1.c). These holes may occur when some sensors in the network manifest unusual behaviors. The assessment of sensors' behaviors would lead to an estimation of the degrees of trust that peers have in each other. To make such estimations, some sensors must be endowed with appropriate mechanisms to weight trust based on data contents, communication pathways, etc. Depending on the application requirements and/or the expected service, trust holes are delimited based on trust weight thresholds. In Fig.1.c, the trust hole is delimited among sensors having trustworthiness weights less or equal to 0.6.

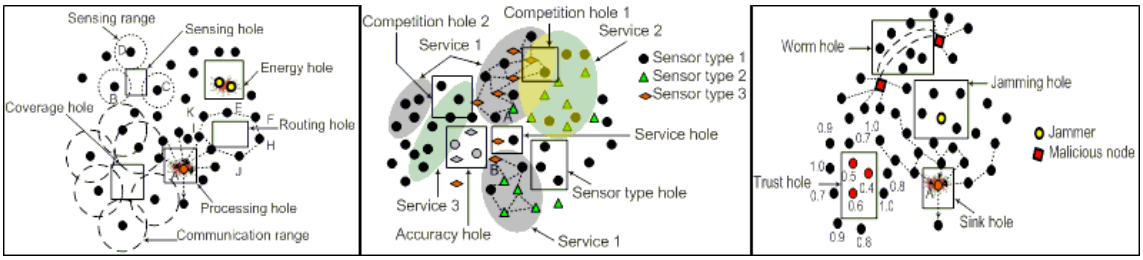

Fig. 1. (a) Physical holes; (b) Semantic holes; (c); Malicious holes.

4. Effects of Holes on Sensor Network

Holes affecting the sensor network activities and performance can be local (they concern the sensor causing the hole) or global (they concern the entire network) [7]. This depends on several parameters such as the locations of holes, the sensors causing the holes, the current context, and the current requirements. In the literature, the effects of holes have been outlined at the level of data acquisition and data routing. At the level of data acquisition, destroyed nodes do not carry out their operations appropriately.

Consequently, some data on events of interest could not be suitably acquired locally from the areas affected by the holes [3]. This local effect may affect the effectiveness of the entire sensor network since the missing information would have been used, for example, for self-adaptation purposes. This is the case when, for instance, a coverage hole preventing the detection of an intruder in a given location may delay the reaction of the network to track that intruder. At the level of data routing, data packets may get stuck in some nodes located at the boundaries of coverage holes [8]. In addition to local effects in terms of energy depletion, global effects are expected on communication pathways particularly due to congestion. In this case, the routing performance of the sensor network may decrease because of potential delays on data traffic, loss of data packets, and data collision [3]. Based on our cause-based taxonomy, holes could be interrelated. For example, trust holes may result in communication and processing overheads to assess the trust weights. These overheads may lead to energy depletion of some sensors. Consequently, energy holes may appear. Due to those holes, coverage holes and semantic holes may occur.

5. Curative Approaches for Sensor Network Holes

The intensive research works that have addressed the issue of holes in sensor networks have particularly focused on four approaches: prevention, detection, repairing, and avoidance. We first survey the main contributions of each approach and then associate then to the causes of anomalies (Table 1).

Preventing holes: To prohibit the appearance of voids within the sensor network, the common idea is to increase the density of the network by deploying redundant sensors, particularly in the threatened areas [9]. Shih et al. [10] have proposed a distributed partition avoidance lazy movement (PALM) protocol for mobile sensor networks. Since sensor movement is the major source of energy consumption, PALM adopts the lazy movement policy for a more effective sensor movement. Huang [11] has proposed a self-deploying method for wireless sensor network where sensors are modeled as ions, and the links between them are treated as ionic bonds. When the number of ionic bonds of a sensor is full, the sensor will expel others out of its field. Sensors organize themselves as the hexagonal format to maximize the network's coverage area, retain the network connectivity, and prevent from introducing the coverage holes. In [12], some guidelines are proposed to prevent the formation of energy holes around sinks by balancing the energy expenditure among sensors. This is achieved by selecting proper sizes of coronas around the sink.

Detecting holes: Funke [1] has proposed a distributed algorithm, based on the topology of the communication graph, which identifies nodes near the boundary of the sensor field as well as near holes' boundaries by allowing sensors in the network to find all the iso-geodesic distances. Ghrist and Muhammad [13] have introduced a technique for detecting coverage holes by means of homology, which is an algebraic topological invariant. Corke et al. [7] have proposed two algorithms where holes are detected from distance by using traffic information and locally by the neighbors of the failed nodes. Wood and Stankovic [3] have described a mapping protocol allowing sensor nodes to detect and surround jammers. In the proposed solution, network applications reason about the region as an entity, rather than as a collection of broken links and congested nodes. Szczytowski et al. [14] have proposed proactive distributed energy profiling algorithms for energy holes. The algorithms search for boundary nodes and use them as references to calculate the energy needs of nodes within the hole. Obado et al. [15] have used the Hidden Markov Model Viterbi algorithm to detect worm holes in a localized WSN.

Repairing holes: The intuitive idea of recharging the batteries of sensor nodes remain difficult to impossible, particularly since some sensors could be operating in remote, harsh, and hostile areas. The existing approaches proposed for repairing holes in sensor networks had been particularly based on maintaining k-connectivity (e.g., [16]) and repositioning the network (e.g., [17; 18]).

Avoiding holes: In order to avoid holes during data communication, some solutions (e.g., [19]) have used right-hand rule approaches where data packets tend to be routed along the boundaries of holes. Other solutions [20; 21] have deployed backpressure approach where data packets are pushed back to upstream node and attempt to find another route to destination. Aissani et al. [22] have proposed an approach that uses geometric formulas to obtain the forwarding region of a sender node located at 1-hop from the hole.

Table 1. Classification of some of the existing works

	Preventing	Detecting	Repairing	Avoiding
Physical holes	[9;10;19;11;12]	[1;3;13;10;17;7;14]	[16;17;18]	[19;20;21;22]
Malicious holes	[23;24]	[5;15;24;25;26;27]		[28;29]

We notice that most of research efforts on curative approaches concern physical holes. As for malicious holes, researchers are mostly active in finding ways to detect malicious holes (especially sink holes and black holes). Very few contributions can be found in avoiding, preventing and repairing malicious holes. Research works in logical and semantic holes are almost absent.

6. Conclusion

In this paper we focused on the problem of holes in sensor networks. We proposed a taxonomy which gives a more exhaustive classification of holes. By surveying a large number of papers, we demonstrated that some types of holes (e.g. semantic holes), despite their importance and potential contribution, did not get enough attention from researchers. This could be explained by the fact that sensor networks are still in their early stage of development and thus it is not surprising that most of the research efforts have addressed technical aspects. Indeed, energy saving, routing, coverage problems, and processing concerns had been the main issues that researchers had dealt with in order to make sensor networks functional. Security had also been of big concern for researchers, which explains the number of works on malicious holes. This is probably due to the critical role of security in the overall well-functioning of sensor networks. We believe that an extended solution allowing for synchronized efforts to prevent, detect, heal, and avoid all types of holes will be necessary in the near future. The implementation of such solution requires interdisciplinary qualifications and cross-layer solutions.

Acknowledgements

This research has received Research Project Grant Funding from the Research Council of the Sultanate of Oman Research Grant Agreement No (ORG DU ICT 10 003).

References

[1] Funke S. (2005). Topological hole detection in wireless sensor networks and its applications. Proceedings of the 2005 joint workshop on Foundations of mobile computing. Cologne, Germany: ACM.

[2] Ahmed N, Kanthere SS, Jha S. The holes problem in wireless sensor networks: a survey. SIGMOBILE Mob. Comput. Commun. Rev. 2005; 9:4-18.

[3] Khan I, Mokhtar H, Merbati M. An Overview of Holes in Wireless Sensor Networks. 11th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting (PGNET), 2010.

[4] Huang CF, Tseng YC. The coverage problem in a wireless sensor network. Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications. San Diego, CA, USA, 2003.

[5] Wood AD, Stankovic JA. Denial of Service in Sensor Networks. *Computer*, 2002; 35:54-62.

[6] Jabeur N, Graniero P, McCarthy J, Xing X. A Knowledge-Oriented Meta-Framework For Integrating Sensor Network Infrastructures. *International Journal of Computers & Geosciences*, 2009; 35: 809-819

[7] Corke P, Peterson R, Rus D. Finding Holes in Sensor Networks. IEEE Workshop on Omniscient Space: Robot Control Architecture Geared toward Adapting to Dynamic Environments, ICRA 2007.

[8] Fang Q, Gao J, Guibas LJ. Locating and bypassing routing holes in sensor networks. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2004.

[9] Liu AF, Wu XY, Gui WH. Research on Energy Hole Problem for Wireless Sensor Networks Based on Alternation between Dormancy and Work. The 9th Inter. Conf. for Young Computer Scientists, ICYCS 2008.

[10] Shih KP, Chen HC, Tsai JK, Li CC. PALM: A Partition Avoidance Lazy Movement Protocol for Mobile Sensor Networks. IEEE Wireless Communications and Networking Conference, 2007.

[11] Huang SC. Ion-6: A Positionless Self-Deploying Method for Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, vol. 2012.

[12] Olariu S, Stojmenovic I. Design Guidelines for Maximizing Lifetime and Avoiding Energy Holes in Sensor Networks with Uniform Distribution and Uniform Reporting. 25th IEEE Int Conf on Comp. Com. 2006, Barcelona, Spain

[13] Ghrist R, Muhammed A. Coverage and hole-detection in sensor networks via homology. Proceedings of the 4th international symposium on Information processing in sensor networks. Los Angeles, California, 2005. IEEE Press.

[14] Szczytowski P, Khelil A, Suri N. LEHP: Localized energy hole profiling in Wireless Sensor Networks. IEEE Symposium on Computers and Communications (ISCC), Riccione, Italy, 2010.

[15] Obado V, Djouani K, Hamam Y. Hidden Markov Model for Shortest Paths Testing to Detect a Wormhole Attack in a Localized Wireless Sensor Network. Procedia CS, 2012; 10: 1010-1017.

[16] Bredin JL, Demaine ED, Hajoaghayi M, Rus D. Deploying sensor networks with guaranteed capacity and fault tolerance. Proc. of the 6th ACM int. symposium on Mobile ad hoc networking and computing. Urbana-Champaign, IL, USA, 2005.

[17] Dini G, Pelagatti M, Savino IM. An algorithm for reconnecting wireless sensor network partitions. Proceedings of the 5th European conference on Wireless sensor networks. Bologna, Italy, 2008. Springer-Verlag.

[18] Sekhar A, Manoj BS, Murthy CSR. Dynamic Coverage Maintenance Algorithms for Sensor Networks with Limited Mobility. Proc. of the Third IEEE Int. Conf. on Pervasive Computing and Communications, 2005. IEEE Computer Society.

[19] Fang Q, Gao J, Guibas LJ. Locating and bypassing holes in sensor networks. *IEEE Mobile Networks and Applications*, 2006; 11: 187–200.

[20] Yu F, Lee E, Choi Y, Park S, Lee D, Tian Y, Kim SH. A modeling for hole problem in wireless sensor networks. Proc. of the 2007 inter. Conf. on Wireless communications and mobile computing. Honolulu, Hawaii, USA, 2007. ACM.

[21] Jia W, Wang T, Wang G, Guo M. Hole Avoiding in Advance Routing in Wireless Sensor Networks. IEEE Wireless Communications and Networking Conference (WCNC), 2007.

[22] Aissani M, Mellouk A, Badache N, Saidani B. Oriented Void Avoidance Scheme for Real-Time Routing Protocols in Wireless Sensor Networks. IEEE Global Telecommunications Conference, New Orleans, 2008. pp. 1 - 5.

[23] Altisen K, Devismes S, Lafourcade P, Ponsonnet C. Analysis of random walks using tabu lists. 19th International Colloquium, SIROCCO 2012, Reykjavik, Iceland, LNCS 2012; 7355: 245-266.

[24] Karlof C,Wagner D. (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Journal of Ad Hoc Networks, Elsevier, 2003; 1(2-3): 293-315.

[25] Sheela D, Naveen KC, Mahadevan G. A non cryptographic method of sink hole attack detection in wireless sensor networks. International Conference on Recent Trends in Information Technology (ICRTIT), 2011.

[26] Tumrongwittayapak C,Varakulsiripunth R. Detecting sinkhole attack and selective forwarding attack in wireless sensor networks. Proc. of the 7th int. conf. on Information, communications and signal processing. Macau, China, 2009.

[27] Misra S, Bhattarai K, Xue G. BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. IEEE International Conference on Communications (ICC), Kyoto, 2011, pp.1 - 5

[28] Baadache B, Belmehdi A. Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks. Journal of Computer Science and Information Security, 2010;7: 10-16.

[29] Teng L, Zhang Y. SeRA: A Secure Routing Algorithm Against Sinkhole Attacks for Mobile Wireless Sensor Networks. 2nd International Conference on IEEE Computer Society Computer Modeling and Simulation, 2010.